2. establishing a document to be signed by the server system; and

3. providing an input means for a user of the client system to confirm an intent to sign the document using an encryption device of the server as an act of signature by the user of the client system; and

b. under control of the server system,

a1 cont.

1. providing a means to control access by categories of client users and to determine whether a particular user is authorized to sign;

B

2. providing a means to uniquely identify the document to be signed that includes a reference to the identifier furnished by the client system; and

3. providing a means to electronically sign a document and its identifier using the encryption device of the server system at the request of a signer,

whereby the document is electronically signed by a client user without the need for a client-side digital certificate or a signature tablet connected to the client user's system.

21. The method of claim 20 wherein the unique identifier of the document includes a sequence of a combination of the client system's computer network location identifier together with the current date and time as reported by the server's clock.

22. The method of claim 20 wherein the method of the server system to authenticate a user requires the client user to supply a biometric identifier to the server system.

23. The method of claim 20 wherein a means is provided for

1. the storage of each unique document identifier in a database at or accessible to the server as a record of each signature transaction;

2. a query of one or more of a collection of unique document identifiers or properties at the server system; and

3. viewing of a record containing information about a signer that is accessible via the unique document identifier or properties,

whereby the existence of a unique document identifier can be further established as authentic by its presence in the database.

a1
con't

B

24. The method of claim 20 wherein a user action is the speaking of a sound.

25. The method of claim 20 wherein a unique document identifier includes an approval for a credit card transaction by a credit card payment system.

26. The method of claim 20 wherein a client side signature device is used to resign the electronic document as a final act of signature intent.

27. The method of claim 20 wherein the client system user is an electronic process or agent.

28. The method of claim 20 wherein the server's encryption device consists of a unique encryption key, generated from a symmetric cipher using the unique document identifier of a document as the character input of a password for generation of the key,

whereby each document to be signed is encrypted with a unique symmetric key, and whereby a cryptotransformation of a document involving the application of such key constitutes its signature.

29. The method of claim 20 wherein the method of the server system to authenticate a user requires the client user to demonstrate knowledge of a secret,

whereby a username and passphrase, username and password, or personal identification number or other knowledge based system can be used to control access by a client user to a server's signature device.

30. A method of electronically signing an electronic transaction record, document, filing, message, binary file or other digital information (hereinafter collectively referred to as "a document" or "the document"), comprising:

a' amt

(a) providing a signature encryption means at a server computer,

B

(b) providing a means of identifying a user,

(c) providing an authentication means of access control for determined classes of users,

(d) providing a document template, with spaces to be filled in with character input by a client user,

(e) providing a character input means by which the client user can remotely provide, and as appropriate, review and correct a series of characters that are to be inserted at spaces within a template, in order to assemble a document that includes specific information furnished by the client user,

(f) providing a means for establishing a unique identifier for the document to be signed which includes an identifier of the client user and the current date and time of the server's system clock,

(g) providing a means by which said client user remotely causes the encryption device to affix an electronic signature to the particular document and identifier that was assembled, whereby documents are created and signed by users using one or more templates and encryption devices located at a remote server over a computer network, including the Internet

31. The method of claim 30 wherein the document to be signed includes formatting tags or codes,

whereby the document can be read by applications that employ such tags or codes after completion and signature.

a' con't

32. The method of claim 30 wherein the document to ~~be signed~~ includes server-supplied text or graphical information that is displayed to the client user but cannot be modified or deleted by the user,

B

whereby signature by the client user indicates acceptance and agreement to the supplied text and graphical information as part of the signed document information.

33. The method of claim 30 wherein the server's encryption device consists of a unique encryption key, generated from a symmetric cipher using the unique document identifier of a document as the character input of a password for generation of the key,

whereby each document to be signed is encrypted with a unique symmetric key, and whereby a cryptotransformation of a document involving the application of such key constitutes its signature.

34. The method of claim 30 wherein the client user performs actions by the speaking of a sound.

35. The method of claim 30 wherein the signed document is an envelope for the transmission and routing of other files, each of which may be included, attached, and/or digitally signed using the method of claim 20.

36. A server system for signing a transaction record, document, filing, message or other communication comprising:

a. an authentication component including:

1. a data storage medium storing information for a collection of users;
2. a receiving component for receiving requests to sign a transaction record, document, filing, message or other communication,

b. an approval component that retrieves from the data storage medium information for the indicated signer, compares it with information provided for the current transaction, and that approves or denies access by the indicated signer to the signature device of the server system;

a1
cont

c. a document creation component that allows a user to enter data in a document template as part of the process to generate a finalized document for signature,

a1

d. an identification component that generates a unique identifier for the document to be signed, which includes an identifier of the client user and the current date and time of the server's system clock; and

f. a signature component consisting of an encryption signature device at the server;

whereby documents can be generated and signed at a server computer by a client user as the client user's own signature without the need for a digital certificate or signature tablet at the client user's computing device.

37. The method of claim 36 wherein any one or more of a collection of authentication means is used to control access by signers to the encryption signature device of the server,

whereby biometric identifiers, usernames and passwords, passphrases, or personal identification numbers, smart cards, or any combination of them or other methods of authentication may be used for signature control purposes.